UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/726,841	12/02/2003	John Hines	127-0013	5556

22120 7590 10/28/2009

ZAGORIN O'BRIEN GRAHAM LLP
7600B NORTH CAPITAL OF TEXAS HIGHWAY
SUITE 350
AUSTIN, TX 78731

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	**PAPER NUMBER**
2436	

MAIL DATE	DELIVERY MODE
10/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/726,841	HINES ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed 6-18-2009.

2. Claims **3 - 23** are pending. Claims **21, 22** have been amended. Claims **1, 2** have been cancelled. Claims **3, 11, 16, 21** are independent. This application was filed 12-2-2003.

Response to Arguments

3. Applicant's arguments have been fully considered but were not persuasive.

3.1 The specification objection has been withdrawn based on specification amendments.

3.2 Applicant argues that the referenced prior art does not disclose, *multiple references and 103 rejection. (Remarks Page 8)*

The MPEP allows the Examiner to utilize a combination of prior art references to reject a claimed invention. The rejection must include a motivation for each combination created based on a set of prior art references and the citation from the combined prior art references must successfully reject each claim limitation.

3.3 Applicant argues that the referenced prior art does not disclose, *hash of a delta CRL. (Remarks Page 9)*

Zhou prior art discloses Certificate Revocation List (CRL) information processing using a delta or subset of CRL information instead of the entire set of CRL information.

(see Zhao col. 5, lines 24-32: delta CRL is returned and processed by appending its entries to current CRL (resultant state CRL)) CRL information processing using a partial or subset of the certificate revocation list is not novel and is disclosed by the current set of prior art.

Van-Oorschot prior art also discloses the concept of a delta CRL in addition to the explicit generation of a subset or segment of the entire CRL based on a specific parameter such as a date (i.e., (CRL (t) state; t for time) or the total size of CRL information. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)) Van Oorschot prior art discloses the concept and usage of a hash value. (see "Van-Oorshcot" col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

Williams prior art discloses the generation and processing of delta (subset) CRL information. And, Williams discloses the generation and usage of a hash value for the secure transfer of message data between two network-connected systems. The message data can be certificate processing information such as CRL information (CRL state or resultant CRL state). (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed); paragraph [0062],

lines 1-7: generate receiving side message data (delta CRL information) hash value; compares sending side message data hash value with receiving side message data hash value)

3.4 Applicant argues that the referenced prior art does not disclose, *the generation of first and second hash values. (Remarks Page 11, 12)*

Van-Oorschot prior art discloses a CRL value generated based on a segment of a CRL based on a function parameter. In addition, VanOorschot discloses the concept and usage of a hash value. And, Williams discloses the generation of hash value(s) using a set of message data such as delta CRL information passed between network-connected systems.

3.5 Applicant argues that the referenced prior art does not disclose, *generation of a hash over a resultant CRL state. (Remarks Page 11, 12)*

Van-Oorschot discloses the generation of a segment or delta CRL based on a parameter (resultant CRL based on t or t+1) as stated above. Van-Oorschot discloses the concept and usage of a hash values as stated above. And, Williams discloses the generation of a hash value of transferred message data such as delta CRL information as stated above.

3.6 Williams prior art discloses wherein a hash generated from message data such as certificate type information including certificate revocation information. Williams prior art discloses a list of key certificates, which have revocation information included for a CRL list. The generated list can be a full or partial list of CRL revocation information or

a delta CRL. (see Williams paragraph [0021], lines 17-20: delta CRL (updated certificate revocation information); paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (CRL information) and corresponding digital signature (including a hash value); paragraph [0062], lines 1-7: generate receiving side message data (delta CRL information) hash value; compares sending side message data hash value with receiving side message data hash value)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **3 - 20, 23** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Zhao et al.** (US Patent No. **7,124,295**) in view of **Van Oorschot et al.** (US Patent No. **5,699,431**: referred to as "Van Oorschot") and further in view of **Williams** (US PGPUB No. **20050021969**).

With Regards to Claim 3, Zhao discloses a method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

b) computing an update to a local certificate revocation list state by applying the

received delta CRL to produce a resultant local CRL state; (see Zhao col. 5, lines 24-32: delta CRL is returned and processed by appending its entries to current CRL (resultant state CRL))

Zhao discloses wherein receiving a delta coded update to a certificate revocation list (a delta CRL) together with an associated first hash value, the delta CRL encoding an update to a preceding certificate revocation list state CRL(t). (see Zhao col. 3, lines 5-10: CRL spanning from most recent CRL to the current CRL; updated delta CRL)

Zhao does not specifically discloses the first hash value computed as a function of at least a resultant state CRL(t+1) computable by applying the delta CRL to the CRL(t) state, and a second hash value as a function of at least the resultant local CRL state and comparing the second and first hash values.

However, "Van Oorschot" discloses:

a) receiving an associated first hash value, the first hash value computed as a function of at least a resultant state CRL(t+n) computable by applying the delta CRL to the CRL(t) state; c) by computing a second hash value as a function of at least the resultant local CRL state (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment

(delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

And, Williams discloses:

c) validating the update at least in part by comparing the second and first hash values. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed); paragraph [0062], lines 1-7: generate receiving side message data (delta CRL information) hash value; compares sending side message data hash value with receiving side message data hash value)

It would have been obvious to one of ordinary skill in the art to modify Zhao-"Van Oorschot" for comparing the second and first hash values as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 4, Zhao discloses the method of claim 3, further comprising: requiring, as a condition precedent to the update, that a transmission that conveys the delta CRL include a valid digital signature establishing a trusted source thereof. (see Zhao col. 5, lines 39-41: signature attached to delta CRL)

With Regards to Claim 5, Zhao discloses the method of claim 3. (see Zhao col. 3, lines 5-10: delta CRL processing system)

Zhao does not specifically disclose whereby the first hash value is computed as a function of both the CRL(t) and CRL(t+n) states, and wherein the second hash value is computed as a function of both a prior local CRL state and the resultant local CRL state. However, "Van Oorschot" discloses wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+1) states, and wherein the second hash value is computed as a function of both a prior local CRL state and the resultant local CRL state. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art

would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46) —

With Regards to Claim 6, Zhao discloses the method of claim 3, further comprising: requesting a CRL update, the request indicating a base t beyond which update is desired; and receiving in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together. (see Zhao col. 3, lines 5-10: request/response for update CRL; Figure 4; col. 5, lines 4-9: multiple delta CRLs)
Zhao does not specifically disclose whereby respective associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of a respective resultant certificate revocation list (CRL) state.
However, "Van Oorschot" discloses wherein respective associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of a respective resultant certificate revocation list (CRL) state. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates

revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

With Regards to Claim 7, Zhao discloses the method of claim 6. (see Zhao col. 3, lines 5-10: delta CRL generation system)

Zhao does not specifically disclose whereby each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived.

However, "Van Oorschot" discloses wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

With Regards to Claim 8, Zhao discloses the method of claim 6, further comprising: performing successive updates to the local certificate revocation list state by applying successive ones of the delta CRLs received in response to the request; and validating the successive updates based on the respective associated hash values. (see Zhao col. 5, lines 4-9: multiple deltas CRLs)

With Regards to Claim 9, Zhao discloses the method of claim 6, wherein the base t is a temporal index. (see Zhao col. 1, lines 17-19: is a time index for certificate revocation)

With Regards to Claim 10, Zhao discloses the method of claim 3, further comprising: if the validating is unsuccessful, requesting a complete copy of a current certificate revocation list. (see Zhao col. 5, lines 27-30: transfer complete copy of CRL (updates appended to previous CRL, entire CRL)

With Regards to Claim 11, Zhao discloses a method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

a) preparing a first delta coded update to a certificate revocation list (a first delta CRL), the first delta CRL encoding an update sufficient to produce a subsequent certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t); (see Zhao col. 3, lines 5-10: updated information (delta CRL) for CRL (first, second)

Zhao discloses wherein transmitting the delta CRL, and a base t. (see Zhao col. 3, lines 5-10: delta CRL transmitted in reply to request; col. 1, lines 17-19: base t (temporal) processing for delta information)

Zhao does not specifically disclose whereby computing an associated first hash value as a function of at least the CRL(t+1) state, and transmitting the associated first hash value in response to a request for certificate revocation list update.

However, "Van Oorschot" discloses:

b) computing an associated first hash value as a function of at least the CRL(t+n) state; (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment

restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

And, Williams discloses:

c) transmitting the associated first hash value in response to a request for certificate revocation list update beyond a base t. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value))

It would have been obvious to one of ordinary skill in the art to modify Zhao-"Van Oorschot" to process hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 12, Zhao discloses the method of claim 11. (see Zhao col. 3, lines 5-10: delta CRL processing system)

Zhao does not specifically disclose whereby the first hash value is computed as a function of both the CRL(t) and CRL(t+n) states.

However, "Van Oorschot" discloses wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+1) states. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46

With Regards to Claim 13, Zhao discloses the method of claim 11, further comprising: receiving a CRL update request indicating a base t beyond which update is desired; and transmitting in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together with respective. (see Zhao col. 3, lines 5-10: delta CRL request/response; col. 1, lines 17-19: base t (time index) processing; col. 5,

lines 4-9: multiple delta CRLs)

Zhao does not specifically disclose whereby associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of at least a respective resultant certificate revocation list (CRL) state from which the associated delta CRL is derived.

However, "Van Oorschot" discloses wherein associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of at least a respective resultant certificate revocation list (CRL) state from which the associated delta CRL is derived. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

With Regards to Claim 14, Zhao discloses the method of claim 13. (see Zhao col. 3, lines 5-10: delta CRL processing system) Zhao does not specifically disclose whereby each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived. However, "Van Oorschot" discloses wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

With Regards to Claim 15, Zhao discloses the method of claim 13, further comprising:

a) performing successive updates to the local certificate revocation list state by

applying successive ones of the delta CRLs received in response to the request; (see Zhao col. 5, lines 4-9: update CRL information with multiple delta CRLs) and

Zhao does not specifically disclose whereby validating the successive updates based on comparison of the associated hash values with respective locally computed hash values.

However, Williams discloses:

b) validating the successive updates based on comparison of the associated hash values with respective locally computed hash values. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed); paragraph [0062], lines 1-7: generate receiving side message data (delta CRL information) hash value; compares sending side message data hash value with receiving side message data hash value)

It would have been obvious to one of ordinary skill in the art to modify Zhao to compare hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 16, Zhao discloses a system comprising:

a) first and second validation authorities (VAs) communicatively coupled to propagate certificate revocation list (CRL) information; (see Zhao col. 2, lines 44-46: certification authority (validation authorities))

Zhao discloses wherein the first VA configured to prepare delta CRLs in correspondence with updates from a certificate authority (CA), each delta CRL encoding a respective update sufficient to produce a next certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t); (see Zhao col. 2, lines 44-46: multiple Certificates Authorities (VAs); col. 3, lines 5-10: generate a delta CRL based on a request) And, Zhao discloses wherein the second VA configured to receive the delta CRLs from the first VA, to calculate based thereon updates to local certificate revocation list states by applying the received delta CRL to produce a resultant local CRL state. (see Zhao col. 2, lines 44-46: multiple Certificate Authorities (VAs); col. 2, lines 57-62: apply delta CRL to produce resultant CRL)

Zhao does not specifically disclose whereby the first VA further configured to compute respective first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1), and to validate each update based at least in part on comparison of respective first hash values received from the first VA with second hash values computed as a function of respective prior local CRL states and resultant local CRL states.

However, "Van Oorschot" discloses:

b) wherein further configured to compute respective first hash values as a function

of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1) and a hash received from a VA, and computed as a function of respective prior local CRL states and resultant local CRL states. (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

And, Williams discloses:

c) wherein to validate each update based at least in part on comparison of respective first hash values with second hash values. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); paragraph [0062], lines 1-7: generate receiving side message data (delta CRL information) hash value; compares sending side message data hash value with

receiving side message data hash value)

It would have been obvious to one of ordinary skill in the art to modify Zhao to compare hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 17, Zhao discloses the system of claim 16, wherein transmission of a given delta CRL and its associated first hash value are secured using a digital signature. (see Zhao col. 5, lines 39-41: digital signature utilized for security) Zhao does not specifically disclose whereby a first hash value. However, Williams discloses wherein a first hash value. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed))

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate a hash value utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a

certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 18, Zhao discloses the system of claim 16, wherein the delta CRLs and associated first hash values are received via an intermediary. (see Zhao col. 5, lines 24-27: remote server (intermediary) received delta CRLs) Zhao does not specifically disclose whereby first hash values. However, Williams discloses wherein first hash values. (see Williams paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed))

It would have been obvious to one of ordinary skill in the art to modify Zhao for hash values utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

With Regards to Claim 19, Zhao discloses a computer program product encoded in one or more media and including instruction sequences executable on a processor of a system that hosts a validation authority to perform the receiving, computing and validating steps of claim 3. (see Zhao col. 6, lines 33-41: software implementation, instructions)

With Regards to Claim 20, Zhao discloses a computer program product encoded in one or more media and including instructions sequences executable on a processor of a system that hosts a validation authority to perform the preparing, computing and transmitting steps of claim 10. (see Zhao col. 6, lines 33-41: software implementation, instructions)

With Regards to Claim 23, Zhao discloses the method of claim 3, further comprising:

a) preparing the delta coded update to the certificate revocation list, the delta CRL encoding an update sufficient to produce the resultant state CRL(t+1) from the preceding certificate revocation list state CRL(t); (see Zhao col. 3, lines 5-10: CRL spanning from most recent CRL to the current CRL; updated delta CRL)

Zhao does not specifically disclose computing the associated first hash value as a function of at least the resultant state CRL.

However, "Van Oorschot" discloses:

b) computing the associated first hash value as a function of at least the resultant state CRL(t+1); (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

And, Williams discloses:

c) transmitting the delta CRL and the associated first hash value in response to a request for certificate revocation list update beyond a base t. (see Williams paragraph [0021], lines 17-20: delta CRL (updated certificate revocation information); paragraph [0023], lines 11-16; paragraph [0024], lines 1-3: receive message (delta CRL information) and corresponding digital signature (including a hash value); (certificate information, signed)

It would have been obvious to one of ordinary skill in the art to modify Zhao-"Van Oorschot" to process hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by Williams. One of ordinary skill in the art would have been motivated to employ the teachings of Williams in order to utilize more efficient systems, methods, computer program products, and data structures for validating a certificate would be advantageous. (see Williams paragraph [0022], lines 22-25)

6. Claims **21, 22** are rejected under 35 U.S.C. 103 (a) as being unpatentable over

Zhao in view of **"Van Oorschot"**.

With Regards to Claim 21, Zhao discloses a tangible computer readable medium encoding, at least transiently, and comprising:

a) delta coded certificate revocation list (CRL) update data that allows a receiving validation authority to generate an updated CRL by applying the delta coded CRL update to a previous CRL state; (see Zhao col. 3, lines 5-10: generate a delta CRL list)

c) a digital signature establishing identity of a source of the computer readable encoding. (see Zhao col. 5, lines 39-41: digital signature appended)

Zhao does not specifically discloses whereby a self-validating indicator encoding a hash computed not as a function of the delta coded CRL update itself, but rather as a function of the next certificate revocation list state CRL(t+n) which may be generating by applying the delta coded CRL update to a previous certificate revocation list state CRL(t).

However, "Van Oorschot" discloses:

b) a self-validating indicator encoded in association with the delta coded CRL update, the self-validating indicator encoding a hash computed not as a function of the delta coded CRL update itself, but rather as a function of the next certificate revocation list state CRL(t+1) which may be generating by applying the delta coded CRL update to a previous certificate revocation list state CRL(t); (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4,

lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

With Regards to Claim 22, Zhao discloses the computer readable medium of claim 21. (see Zhao col. 3, lines 5-10: delta CRL information processing system)
Zhao does not specifically disclose whereby the encoded hash is computed as a function of both the next state CRL(t+1) and the previous state CRL(t).
However, "Van Oorschot" discloses wherein the encoded hash is computed as a function of both the next state CRL(t+n) and the previous state CRL(t). (see "Van Oorschot" col. 4, lines 27-28: "delta: mechanism (delta CRL); col 4, lines 36-41: delta CRL; a list of revoked certificates subsequent to date of most recent previously issued such revocation list; col. 5, lines 14-16: in a certificate identifying one or more CRL

segments (delta CRL(s)); col. 5, lines 30-41: address_field value contains one-way hash of an address_list value; address_list value equals reason specific CRL segment (delta CRL); segment restricted to entries corresponding to certificates revoked)

It would have been obvious to one of ordinary skill in the art to modify Zhao to generate hash value(s) utilizing a subset of PKI certificate information such as a delta set of revoked certificates as taught by "Van Oorschot". One of ordinary skill in the art would have been motivated to employ the teachings of "Van Oorschot" in order to provide an efficient method of selective processing and use of CRLs by means of prioritized CRLs. (see "Van Oorschot" col. 2, lines 44-46)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
October 13, 2009